SAFE ON SOCIAL
TRAINING AND EDUCATION

Identifying common social media and cyber security risks and threats

www.safeonsocial.com

Identifying common social media and cyber security risks and threats

As a valuable member of our school's staff, it's essential to be aware of the potential risks and threats that can impact our organisation through social media and cyber security. Here are some of the most common risks and threats that you should keep in mind:

Phishing Scams: Cyber attackers often use phishing scams to trick employees into revealing sensitive information such as login credentials, credit card details, or other personal data. These attacks can occur via email, social media messages, or other online channels.

Malware: Malware is a type of software that is designed to damage, disrupt or gain unauthorized access to a computer system. Malware can be spread through social media links, downloads, or email attachments.

Ransomware: Ransomware is a type of malware that encrypts the files on a computer system, making them inaccessible to users until a ransom is paid to the attacker.

Social Engineering: Social engineering is a technique used by attackers to manipulate people into divulging sensitive information or performing actions they wouldn't normally do. Attackers can use social media to gather information about employees and use that information to create convincing phishing emails or other social engineering attacks.

Data Breaches: A data breach occurs when an attacker gains unauthorised access to a company's data. This can happen through social media, phishing scams, or other cyber-attacks.

Insider Threats: Insider threats occur when an employee intentionally or unintentionally compromises company data. This can happen through social media posts that reveal sensitive information or through intentional or accidental sharing of login credentials.

To help protect our school from these risks and threats, here are some steps that you can take:

Stay Informed: Attend training sessions, read school policies, and stay informed of industry news to keep up-to-date with the latest security risks and threats.

Use Strong Passwords: Use strong, unique passwords for each of your accounts, and never share your login credentials with anyone.

Be Cautious of Links and Attachments: Be careful when clicking on links or downloading attachments, especially if they are from unknown sources or look suspicious.

Follow Security Policies: Adhere to school security policies, including guidelines for handling sensitive information, using strong passwords, and reporting security incidents.

Report Suspicious Activity: If you notice any suspicious activity on your accounts or suspect a security breach has occurred, report it immediately to your IT department or manager.

By being aware of these common social media and cyber security risks and threats and taking steps to protect our school, you can help prevent potential damage to our data and reputation. Thank you for your commitment to keeping our school safe and secure.